Calculating Conditional Core Damage Probabilities for Nuclear Power Plant Operations

Curtis L. Smith
Idaho National Engineering and Environmental Laboratory
Idaho Falls, Idaho 83201

ABSTRACT

A part of managing nuclear power plant operations is the control of plant risk over time as components are taken out of service or plant upsets are caused by initiating events. Unfortunately, measuring risk over time proves to be challenging, even with modern PRAs and PRA tools. In general, the process of measuring the operational risk would satisfy three desires: (1) the measurement would provide the risk magnitude for a particular event or over a period of time; (2) the risk results could be summed for a period of time to obtain a cumulative risk profile; and (3) the measurement process would be tractable while still using the current modeling techniques and tools. This paper demonstrates the calculation of the conditional core damage probability (CCDP) for the two cases of component outages and initiating events. In addition, two potential complications were identified that must be addressed when performing a CCDP calculation. The first complication, determining the appropriate nonrecovery probabilities to be applied to an inoperable component or initiating event, addresses the possibility of the plant operators preventing damage to the plant from their actions. The second complication, adjusting common-cause probabilities specific to the plant configuration, accounts for the fact that the PRA common-cause probabilities built into the model are applicable only during nominal conditions. The examples presented in the paper illustrate the potential underestimation in CCDP when modifications to common-cause probabilities are ignored. These underestimation errors ranged from a factor of two to over a factor of six underestimation in CCDP.

KEYWORDS

risk analysis, core damage frequency, core damage probability, risk monitor, common-cause failure, recovery, plant operation, risk profile

NOTE: This paper is the pre-print version of the paper published in *Reliability Engineering and System Safety*. For the published paper, please see RESS **59** (1998) pp. 299-307.

1 INTRODUCTION

During the operation of a nuclear power plant, conditions exist that alter the risk of operating the facility. These conditions (or events) that result in a change, where "change" can be either an increase or decrease in risk, fall under three general categories. First, plant activities dictate that certain components will be incapable of performing their desired functions at certain times during operation. Examples of these activities that incapacitate components include preventative maintenance and testing (both scheduled activities), corrective repairs to failed components (an unscheduled activity), and Technical Specification actions such as either entering a Limiting Condition of Operation to replace a component or performing specified functional tests (these activities could be either scheduled or unscheduled). Second, improper plant design or maintenance could result in an unintended reduction in plant or component reliability, potentially over long periods of time. Examples of these reductions in plant reliability include faulty component design such as undersized valve motor operators[1] and insufficient fire-barrier protection[2] or faulty component restoration and testing after a maintenance activity. Third, initiating events that occur during operation cause challenges to plant systems and operators. Examples of these events include losses of off-site power, miscellaneous plant transients, and loss-of-coolant pipe breaks.

While it is readily acknowledged that operational plant risk changes over time as components are taken out of service or plant upsets are caused by initiators, measuring the risk over time proves to be challenging. Ideally, the process of measuring the operational risk would satisfy three desires:

1. The risk measurement would allow the analyst to calculate the risk magnitude for a particular event or over a period of time.

2. The risk results would be consistent such that the results could be summed for an operational period of time (e.g., a single 18 month fuel cycle) to obtain a cumulative risk profile over a period of interest.

3. The risk measurement process would be tractable and represent the actual risk while still using the current modeling techniques, tools, and state of knowledge.

The focus of this paper is to demonstrate a risk measurement method that can quantify operational plant risk while satisfying all three of the desires listed above. The second section of this paper describes the risk measure that is the most appropriate for calculating operational risk and provides justification for its use as a risk measure. The third section discusses the risk calculation to be performed when plant components are rendered inoperable through one of the mechanisms discussed previously. The fourth section presents the risk calculation to be performed when an initiating event occurs during the period of interest. The fifth section provides a summarization of the major points raised in the paper along with suggestions aimed at improving the operational risk measurement process.

2 OPERATIONAL RISK MEASURE

Within the scope of probabilistic risk analysis (PRA), numerous "risk measures"[a] are available as a direct output from the PRA tools currently in use. These measures include the core damage frequency, the probability of core damage, the *percent* increase (or decrease) in core damage, and a *factor* increase (or decrease) in core damage frequency. Traditionally, measures using the core damage frequency as the basis of the measure have been the focus for activities related to risk-informed regulation. For example, the paper by Fleming[3] discusses a risk monitor core damage frequency and the difficulties that arise when trying to estimate an instantaneous core damage frequency. Further, the core damage frequency result is readily available from current PRA tools. Also, the core damage frequency measure provides an approximate estimate of the risk magnitude for a particular event. But, this measure does not satisfy all three of the desirable attributes. Specifically, the core damage frequency measure will not differentiate between two operational events that have the same core damage frequency but exist for different durations. Further, the core damage frequency measure can not be summed over an operational period of time to obtain an overall risk measure.

Since the core damage frequency is not an appropriate measure for tracking risk over a known time period, another measure must be considered. This measure, a conditional core damage probability (CCDP), turns out to satisfy all three of the desirable attributes discussed previously. In addition, the CCDP make use of the core damage frequency, thereby providing a bridge of understanding for those analysts familiar with using the core damage frequency measure.

For the CCDP measure, the element of time is incorporated into the calculation, allowing the analyst to estimate the risk magnitude for an event at a certain point in time (e.g., at the time of an initiating event) or for a condition existing over a length of time (e.g., an improperly installed valve that remains unnoticed). Since the CCDP is dimensionless (it is a probability) and factors in time if necessary, two different events can be compared quantitatively to one another. Thus, the first desirable risk measure attribute is satisfied. This consistency in the risk measure from one event to the next allows for the integration over the time period of interest to obtain an overall risk profile. Consequently, the second desirable risk measure attribute is satisfied. Finally, since the calculation of the CCDP builds upon the core damage frequency, additional risk models and analysis tools are *not* required; accordingly, the third desirable attribute is satisfied.

The remainder of this paper provides the theory behind and examples of the CCDP calculation for two types of scenarios. First, the treatment of conditions over a known duration (i.e., a component that is out of service) is addressed. Second, the treatment for the occurrence of an initiating event and its impact on risk is presented. But, prior to the discussion for either of these scenarios, the general philosophy behind calculating an operational risk measure is provided.

The calculation of an operational risk measure attempts to create a risk profile, over time, conditional upon the component outages and plant initiating events that actually occurred during the period of interest. The CCDP is believed to be the best measure as a basis for this risk profile since it has many desirable features. But, what is *not* being calculated for the risk profile is the probability that severe core damage *did* happen. If we look at the operation during the last 12 months for any nuclear power plant in the U.S. and ask "what is the probability that severe core damage did happen," the resulting probability is zero. While a zero probability for severe core damage is of great interest for the plant owners and operators, this particular probability question in itself is of little interest. Instead, the risk profile that deserves attention asks the question:

> What could happen (i.e., what is the probability of core damage) if the conditions and events that existed over the duration of interest were realized at a later time?

Thus, the CCDP that is part of the risk profile measures the likelihood of core damage conditional upon the plant configuration and operating status at a point in time during the duration of interest. In addition, the conditionality that is imposed on the CCDP only reflects impacts on the measure of interest (i.e., core damage). Such impacts include the scenarios that have been discussed (e.g., a component outage or the occurrence of an initiating event). Situations where a component *operates* are not factored into the CCDP calculation. The fact that a particular component operated at a point in time is not important to the calculation. What is important is the question concerning the probability that the operating component *could* have failed. At first glance it may appear that the CCDP calculation is performed using the "relative frequency" statistical framework[4] since the notion of a repeatable plant configuration is implied (i.e., if the plant were in this configuration 100 times, how many times would the operating component fail?). But, the CCDP calculation is still performed using the subjective (or Bayes) framework that forms the foundation of modern PRAs. Nonetheless, the notion of a repeatable configuration may help the reader conceptualize the philosophy behind operational risk profile calculations.

To illustrate the philosophy backing the CCDP calculation, a non-nuclear power plant example will be utilized. To motivate this example, assume that an audience will see a particular magic show. In this show, the magician performs a special magic trick, using a length of rope, that incurs great risk and the potential for death. This trick is performed only once a month, every month of the year. Unfortunately, the type of rope used by the magician varies from one performance to another, depending on the available rope supply. It is known, from collecting rope usage data, that on any given performance, the probability of one type of rope being used during the performance is:

[a] While the term "risk measure" is used, the focus of the paper is on the occurrence, specifically the probability of occurrence, of core damage. Since stopping at core damage does not directly quantify the event consequences, the traditional definition of risk (risk = frequency of event × consequence of event) is not being used. Fortunately, one could extrapolate the concepts presented within this paper to include the evaluation of the event consequence (e.g., Level 2 or Level 3 analysis).

P(best rope | performance) = 0.5
P(good rope | performance) = 0.4
P(bad rope | performance) = 0.1 .

Further, it has been estimated that the probability of the magician dying during the performance varies from 0.1 to 0.001, depending on the type of rope that is used. Specifically, the probability of death is:

P(death | best rope is used) = 0.001
P(death | good rope is used) = 0.01
P(death | bad rope is used) = 0.1 .

The magician insists that "the show must go on" irrelevant of what type of rope is available for a particular performance. Knowing this, one could estimate the probability of death for a given, upcoming performance by the equation:

$$\text{P(death | performance)} = \sum \text{P(death | rope type X is used)} \times \text{P(rope type X is used | performance)} .$$

Evaluating this expression for the three rope types yields:

$$\begin{aligned}\text{P(death | performance)} &= [0.001 \times 0.5] + [0.01 \times 0.4] + [0.1 \times 0.1] \\ &= 0.0005 + 0.004 + 0.01 = 0.0145 .\end{aligned}$$

where it can be seen that using the "bad" rope incurs the greatest amount of risk. Using the bad rope gives a probability of death more than two times that of the good rope and 20 times that of the best rope. While this risk calculation is adequate to determine the risk differences between using the three types of rope, it does not indicate what the risk was for a particular pattern of performances (say over the last 12 months). Instead, what is needed to determine the risk over a specified period of time is a risk profile calculation. To perform this risk profile calculation, the actual rope type used for each of the last 12 shows is needed and are shown below.

Show	1	2	3	4	5	6	7	8	9	10	11	12
Type	good	best	best	best	good	bad	best	good	best	best	good	best

From the previous calculation, the probability of death, given usage of a particular type of rope, is known for each rope type. These probabilities are: P(death | best rope) = 0.001, P(death | good rope) = 0.01, and P(death | bad rope) = 0.1. Plotting these probabilities for each performance over the last 12 months gives Figure 1. If these conditional probabilities are summed over the last twelve performances, a cumulative probability risk profile is constructed. An example of a cumulative risk profile is shown in Figure 2.

The plots shown in Figures 1 and 2 are representations of risk profiles. These risk profiles demonstrate the probability of death that was experienced by the magician for the performances over the last year. The calculation for similar plots will be discussed relevant to the operation of nuclear power plants in the following two sections. First, the issue of component outages, and their impact on the risk profile, is presented. Second, the concern of initiating events and complications to the risk profile calculation is addressed. One important difference between the magician example risk profile and that of an operating nuclear power plant is that the ordinal axis consists of time and is continuous rather than the discrete case (i.e., per performance) above.

The probability that the magician died over the last 12 performances is zero since the magician successfully completed the last performance. But, based upon the calculated risk profiles that are displayed in Figures 1 and 2, we can state that, given the type of ropes used and the number of performances over the year, the probability of death during a performance is about 0.147. As will be demonstrated later, similar statements can be made about the probability of experiencing damage to a nuclear power plant reactor during a component outage or the occurrence of an initiating event.

3 TREATMENT OF COMPONENT OUTAGES

The first scenario to be addressed as part of the risk profile calculation is for the outage of components. The specific cause of the component outage could include any plant activity that prevents a component from performing its desired function (e.g., preventative maintenance, corrective repairs) or improper component design or maintenance resulting in the reduction of component reliability (e.g., faulty design implementation, improper component restoration after maintenance). The identifying attribute for the component outage scenario is that a component is unable to perform its intended function for some duration of time. Typically, component outages of short durations (e.g., less than 5 minutes) are ignored in order to simplify the risk profile analysis.

To calculate the CCDP for a component outage, the conditional core damage frequency must first be calculated. This core damage frequency is conditional upon the component or components that are inoperable. Consequently, one would adjust the plant PRA to reflect the component outages; this adjustment is frequently called "mapping" the scenario into the PRA model. As part of this mapping process, three items must be considered before the conditional core damage frequency can be calculated.

1. Finding the affected basic events in the PRA in order to change their failure probabilities to reflect the inoperable component.

2. Assessing the likelihood that the affected component could be recovered (i.e., returned to an operational state).

3. Determining other impacts on the PRA model such as changes to common-cause failure probabilities and initiating event frequencies.

For the remainder of this paper, assume that a hypothetical power plant has a core damage model that gives us the minimal cut sets (where "·" represents a logical "AND" Boolean operation and "+" represents a logical "OR" Boolean operation)

$$CD = (IE1 \cdot A1 \cdot A2 \cdot A3) + (IE1 \cdot CCF\text{-}A) + (IE2 \cdot A1 \cdot B1) + (IE2 \cdot A1 \cdot B2) .$$

where IE1 = initiating event #1 (nominal frequency = 0.01/yr)
IE2 = initiating event #2 (nominal frequency = 0.001/yr)
A1 = component A1 fails (nominal probability = 0.05)
A2 = component A2 fails (nominal probability = 0.05)
A3 = component A3 fails (nominal probability = 0.05)
CCF-A = common-cause failure of components A1, A2, and A3 [nominal probability = 0.05 × 0.1 × 0.2 = 0.001, using the Multiple Greek Letter (MGL) model[5,6] where β = 0.1 and γ = 0.2]
B1 = component B1 fails (nominal probability = 0.06)
B2 = component B2 fails (nominal probability = 0.06) .

Using the nominal event frequencies and probabilities, the base case core damage frequency has a value of 1.73×10^{-5}/yr.

Once the nominal core damage frequency is known, a CCDP could be calculated for a known duration. For example, if the plant were to be operated in its nominal state for 100 hours, the probability of seeing one or more core damage events over this duration is given as

$$\begin{aligned}(CD \mid 100\ hours,\ nominal\ conditions) &= 1 - e^{-\lambda_{CD}\, t} \\ &= 1 - e^{-1.73\times10^{-5}/yr\,(100\ hr)(1\ yr/8760\ hr)} = 1.97\times10^{-7}\end{aligned}$$

where λ_{CD} = the core damage frequency
t = the time duration.

This evaluation of the CCDP over the 100 hour duration assumes that the core damage scenarios of interest satisfy all of the assumptions of Poisson events.

Since core damage frequencies are readily available from a PRA, the nominal CCDP calculation could be easily performed for any defined duration. Unfortunately, during regular operations of a facility, non-nominal conditions are frequently encountered. These non-nominal conditions complicate the CCDP calculation. The two main complications of the calculation are (1) determining the appropriate nonrecovery probabilities to be applied and (2) adjusting common-cause probabilities specific to the plant configuration. These two complications will be discussed in turn.

Typical PRAs include basic events representing failure of an operator or other plant personnel to repair or recover an inoperable component. These basic events are called "recovery actions" and are quantified by determining the probability that the operator fails to recover or fix the inoperable component. But, in a PRA, these recovery actions are intended to cover the general case of a component failing at any time during the mission time defined for the analysis. Consequently, the nonrecovery probability is an "average" type of value (with associated variability as defined by the uncertainty distribution) and is not specific to a particular component failure. Since the analyst performing the CCDP calculation is going to focus on a particular configuration (and, hence, a particular type of component failure), the predefined nonrecovery probability used for an inoperable component in the PRA may not be suitable for the CCDP calculation.

As an example of the nonrecovery issue, assume that the PRA model uses a diesel generator nonrecovery probability of 0.1. In the results for the PRA, every cut set that contains a diesel generator failure basic event will also contain a diesel generator nonrecovery event. Now, a CCDP calculation to be performed is conditional upon a diesel generator failure that lasted 20 hours. During this 20 hours, the diesel was inoperable and *could not be recovered*. If the analyst were to perform the evaluation by resetting the diesel generator failure basic event to a logical "True" (i.e., guaranteed failed) or a probability of 1.0 and did nothing to the diesel nonrecovery event, the CCDP calculation would be in error. Instead, what the analyst should do is to adjust the diesel nonrecovery probability to an appropriate value specific to the condition, which in this case would be a logic "True" or a probability of 1.0.

The difficult part of the nonrecovery adjustment is determining the appropriate nonrecovery probability for the condition of interest. For the case where a component is failed and cannot be recovered, the probability of nonrecovery is 1.0. If a component is inoperable but could possibly be recovered if necessary, the nonrecovery probability has a value that is less than one. Deciding on the appropriate nonrecovery probability may require a detailed task analysis or human reliability analysis specific to the restoration of the inoperable component. Discussion of the application of a human reliability analysis for a given context can be found in the open literature.[7] Alternatively, an analyst may decide to evaluate several groups of typical restorations activities and then use these "generic" nonrecovery probabilities for future analyses. But, resolution of the nonrecovery issue may require detailed study on its own and is beyond the scope of this paper. The reader is directed toward other applicable human reliability references.[8,9]

The second complication in calculating CCDPs deals with the adjustment of common-cause failure probabilities. Most modern PRAs contain basic events representing common-cause failure for a group (i.e., two, three, or four) of redundant components. For example, if three motor driven pumps are in parallel, and failure of all three pumps is required to fail the entire pumping system, then a common-cause basic event would appear in the fault tree model and would represent failure of all three pumps due to some common failure mechanism. Further, this common-cause basic event may be quantified by use of one of the typical parametric common-cause models such as the MGL or alpha-factor methods.[5] Assuming that this event were quantified with the MGL method, the basic event probability would be found using the equation.

$$P(common\text{-}cause\ \ failure \mid three\ \ components) = Q_t\, \beta\, \gamma \quad .$$

where Q_t = total failure probability of one of individual components
β = conditional probability that the cause of the first component failure will be shared by at least one other redundant component
γ = conditional probability that the cause of the first component failure will be shared by at least two other redundant components.

Note that this calculation for the probability of common-cause failure ignores the terms representing two components failing due to common-cause at the time the third component is inoperable due to an independent failure. But, if one were to quantify both terms, it can be seen that the "Q_t β γ" term kept in the analysis for this paper dominates the ignored term (the "Q_t β γ" term equals 0.001 while the ignored term equals 0.00027). Thus, while some small calculational inaccuracies are introduced by ignoring additional terms, the benefit is that the discussion presented in this paper is less cluttered. Nonetheless, if the analyst desires to express the common-cause failure probability using all of the terms embodied within the basic parameter model, the philosophy discussed in this paper would still be used to condition the basic parameter terms upon the situation of interest.

While the above common-cause method is commonly used in PRA, this quantification of the nominal common-cause failure probability is applicable *only* for the nominal case. During the calculation of a CCDP, additional information is known about the configuration of the plant that could invalidate the nominal common-cause probability. For example, if one of the three pumps were known to be failed, it is not correct to have a minimal cut set representing failure of all three pumps. To fail the entire pumping system after one of the pumps is already failed only requires failure of the *remaining* two pumps. Thus, what would be desirable in the PRA results is the probability that the remaining two components fail due to common cause given one pump has already failed. This conditional probability could be much different (by orders of magnitude) than the original probability of common-cause failure and will depend on the circumstances of the first pump failure and the probabilities of the MGL parameters.

In order to quantify the conditional common-cause probability for a CCDP calculation, one must consider the type of failure or outage experienced by the first pump. The type of failure by the first pump will fall into one of three categories:

1. The pump failed due a common-cause type of failure. This category would include failures that could potentially be identified as common-cause failures.

2. The pump failed due to an independent type of failure. Independent type failures are those failures that clearly do not have the potential to fail multiple, redundant components (i.e., are not common-cause failures).

3. The pump is inoperable due to operator intervention. This category would include outages for testing and preventative maintenance. Not included in this category are outages due to a component failure (component failures belong in either category 1 or 2, depending on the nature of the failure). Consequently, outages to repair a failed component belong in either category 1 or 2.

Once the appropriate category is decided for the specific condition being analyzed, the common-cause probability must be adjusted to reflect the new state of knowledge. First, the case for category 1 will be explored.

If one of the three pumps has failed, and the failure was due to a common-cause (or potential common-cause) mechanism, then the Q_t term in the MGL model should be set to a probability of one. Remember that this term represents the probability of failure of at least one component in our common-cause group. Since we know a component has failed, Q_t has a value of one for this particular situation.[b] In other words, the first pump failure is just the first step in what could have been a common-cause failure of all three pumps. Changing this parameter value (Q_t) from its nominal probability (which, in a typical PRA, could be on the order of 1×10^{-2} to 1×10^{-5} depending on the unreliability of the component in question) to a value of one may have a large impact on the probability of common-cause for the remaining component. For this reason it is critical to adjust the common-cause probabilities during the CCDP calculation to account for the specific state of knowledge. By not adjusting the common-cause probability, an analyst runs the risk of dramatically underestimating the risk of the particular configuration. Consequently, the new probability of common-cause failure for the remaining two pumps can be found by

$$(\textit{common-cause failure} \mid 2 \textit{ components remain}, 1 \textit{ component failed via CCF}) = 1.0\,\beta\,\gamma$$

Again, note that this calculation for the probability of common-cause failure ignores the terms representing two components failing due to common-cause in conjunction with the third component failing due to an independent failure.

For the case of category 2, one of the pumps in our group of three has failed, but the pump did not fail from common-cause impacts. Since the pump is inoperable from an independent failure, it would be incorrect to change the Q_t parameter to a value of one because this first failure is not the first of three potential common-cause failures. In other words, we did not see an event that could have resulted in the common-cause failure of all three pumps. Instead, a possible scenario that could arise after the independent failure of the first pump is to then experience common-cause failure of the

[b] One way to think about this pump failure (and its impact on the probability of all three pumps failing due to common-cause) is to envision the first failure as the first of three potential failures. The other two failures that did not occur during this particular scenario still had the potential to happen based upon the common-cause impact that failed the first pump.

remaining two pumps. But, the probability that two components fail due to common-cause is (assuming that this event were quantified with the MGL method)

$$P(\mathit{common{-}cause\ \ failure} \mid 2\ \ \mathit{components\ remain},\, 1\ \mathit{component\, fails\, independently})\ =\ Q_t\,\beta \quad .$$

Consequently, when one component fails due to an independent failure, the "last remaining" MGL parameter would be set to a probability of one in the nominal common-cause equation. For the case of three components where one experiences an independent failure, the γ parameter would be set to a probability of one. In principle, an independent failure of one redundant component effectively reduces the overall redundancy level by one.

For the case of category 3, we see a situation similar to that discussed for category 2. Disabling one of the pumps for testing and preventative maintenance is an elective process and, as such, effectively reduces the overall redundancy level by one. Thus, the guidance for category 3 is the same as that for category 2. Complicating the category 3 case is the assumption that disabling the pump for test or maintenance activities will make the pump unable to perform its intended function. If the test or maintenance activity could be readily terminated and the pump restored to service, declaring the pump as inoperable may not be correct.

Lastly, before an example calculation is presented for a component outage, the analyst should be aware of other impacts on the PRA model. A common example of a PRA-related impact would be for the case where a component outage affects the frequency of initiating events. If a loss-of-service-water initiating event were modeled in the PRA, a failure of one or more of the service water pumps would increase the likelihood that the service water system would be lost during plant operation. For example, in the Brunswick Individual Plant Examination (IPE), the loss of Nuclear Service Water initiating event was quantified by reevaluating the service water system fault tree. The nominal frequency for this initiating event based upon the fault tree was found to be 3.29×10^{-3}/yr.[10] Loss of either a conventional or nuclear service water pump would increase the nominal initiator frequency above the 3.29×10^{-3}/yr baseline.

To demonstrate the complication of recovery and common-cause issues for the CCDP calculation for component outages, let us return to the hypothetical power plant core damage model. For this example, assume that the A1 component failed due to an intake of air bubbles, causing the component to not function. Further, assume that the component failure falls into the common-cause category 1 since it is a potential common-cause type of failure. The duration of the component outage is 36 hours; during the outage time the failed component is not recoverable. The first step in the CCDP calculation is to quantify the conditional core damage frequency and is given by

$$\begin{aligned}\lambda_{\mathrm{CD}} \quad &= (\mathrm{IE1} \cdot \mathrm{A1} \cdot \mathrm{A2} \cdot \mathrm{A3}) + (\mathrm{IE1} \cdot \mathrm{CCF\text{-}A}) + (\mathrm{IE2} \cdot \mathrm{A1} \cdot \mathrm{B1}) + (\mathrm{IE2} \cdot \mathrm{A1} \cdot \mathrm{B2}) \\ &= [(0.01/\mathrm{yr})(1.0)(0.05)(0.05)] + [(0.01/\mathrm{yr})(0.02)] + [(0.001/\mathrm{yr})(1.0)(0.06)] + \\ &\quad\ [(0.001/\mathrm{yr})(1.0)(0.06)] \\ &= 3.45 \times 10^{-4}/\mathrm{yr}\ .\end{aligned}$$

Given a duration of 36 hours, the CCDP is

$$\begin{aligned}P(CD\ \mid\ 36\ \ \mathit{hours},\ A1\ \ \mathit{failed})\ &=\ 1\ -\ e^{-\lambda_{CD}\,t} \\ &=\ 1\ -\ e^{-3.45\times10^{-4}/yr\ (36\,hr)(1\,yr/8760\,hr)}\ =\ 1.42\times10^{-6} \quad .\end{aligned}$$

The question could be asked "what is the overall impact on the CCDP if the impact on the common-cause probability were ignored?" For this hypothetical example, ignoring the change in the common-cause probability (i.e., CCF-A) results in a conditional core damage frequency value of 1.55×10^{-4}/yr. From this, the CCDP (still for the 36 hours) is 6.37×10^{-7}. Therefore, ignoring the impact on the common-cause probability causes the CCDP to be underestimated by a factor of 2.2. From previous work performed by the author using several U.S. nuclear power plant PRA models and the SAPHIRE risk assessment software,[11] the CCDP underestimation from overlooking the common-cause probability adjustment ranges from negligible to over a factor of ten. Consequently, risk profile calculations that ignore adjustments to common-cause probabilities have the potential to grossly underestimate the plant risk during a particular operating configuration.

4 TREATMENT OF INITIATING EVENTS

The second scenario to be addressed as part of the risk profile calculation is for the occurrence of an initiating event. Included in this scenario are all of the types of initiating events that are modeled in the plant PRA and include: general plant transients (e.g., reactor trips, loss of off-site power, loss of feedwater), loss-of-coolant accidents (e.g., stuck open relief valve, small break loss-of-coolant), and other special transients (e.g., steam generator tube ruptures). The identifying attribute for the initiating event scenario is that one of the potential plant initiating events has happened. In addition, components that are inoperable or fail at the time of the initiating event must be accounted for in the CCDP calculation.

To calculate the CCDP for an initiating event scenario, an analyst must map the event into the PRA model and calculate the CCDP directly. This calculation differs from the component outage case since the conditional core damage frequency is not calculated first and then used to calculate the CCDP. Instead, one would adjust the plant PRA to reflect the specific initiating event that occurred and any component outages. As part of this mapping process, three items must again be considered before the CCDP can be calculated.

1. Finding the affected basic events in the PRA in order to change their failure probability or initiator frequency to reflect the inoperable component(s) and particular initiating event.

2. Assessing the likelihood that any affected component could be recovered (i.e., returned to an operational state).

3. Determining other impacts on the PRA model such as changes to common-cause failure probabilities.

Since the concerns for item numbers 2 and 3 above are the same for both initiating events and component outages and they have already been addressed, the reader is referred back to Section 3 for details. The major difference between an initiating event CCDP calculation and a component outage calculation is in the treatment of the initiator basic events in the PRA model. To demonstrate this difference in the two calculations, let us revisit our hypothetical PRA model. Again, core damage is given by

$$CD = (IE1 \cdot A1 \cdot A2 \cdot A3) + (IE1 \cdot CCF\text{-}A) + (IE2 \cdot A1 \cdot B1) + (IE2 \cdot A1 \cdot B2)\ .$$

In this simple PRA model, two different initiating events are used, IE1 and IE2. For the component outage CCDP calculation in the previous section, both initiator basic events were left at their nominal values in order to determine a conditional core damage *frequency*. Now, for the initiating event case, the basic event that corresponds to the initiating event that actually occurred should be set to a probability of one while all of the other initiator basic events should be set to a probability of zero. Notice that by changing the initiator events from a frequency (i.e., per unit time) to a probability (i.e., either the initiator happened or not), the PRA model calculation will directly express the CCDP.

In addition to setting the initiator basic events to either probabilities of one or zero, an analyst must consider whether or not the initiating event that occurred was reversible (i.e., recoverable). For example, initiating events that are not considered to be reversible include steam generator tube ruptures [the ruptured tube(s) can not be easily plugged] and general transients (the operators can not make the plant "untrip"). Conversely, some initiating events can be reversed and include a loss of off-site power (off-site power may be restored in a short time period) and loss-of-coolant events (pipe breaks could be isolated). For the initiator event that was set to a probability of one, the analyst must determine the probability that the initiator could have been reversed given the same conditions existing at the time of the initiating event. If it is determined that the initiator could not have been reversed, no further changes to the initiator event probabilities are required. But, if it is determined that the initiator may have been reversed, the analyst must decide the probability that the initiator was not reversed, given the initiator occurs (i.e., determine the initiator nonrecovery probability). This nonrecovery probability would then replace the probability of one that was assigned to the initiator event at the start of the analysis.

To demonstrate the CCDP calculation for the initiating event case, assume that the initiator IE1 occurred at the hypothetical plant. Further, assume that the A1 component failed in response to the initiating event due to an intake of air bubbles, causing the component to not function. Also, assume that the component failure falls into the common-cause category 1, since it is a potential common-cause type of failure and it is not recoverable. Now, the CCDP calculation is given by

$$\begin{aligned} P(\mathit{CD} \mid \mathit{IE1\ occurred,\ A1\ failed}) &= (IE1 \cdot A1 \cdot A2 \cdot A3) + (IE1 \cdot CCF\text{-}A) + (IE2 \cdot A1 \cdot B1) + (IE2 \cdot A1 \cdot B2) \\ &= [(1.0)(1.0)(0.05)(0.05)] + [(1.0)(0.02)] + [(0.0)(1.0)(0.06)] + [(0.0)(1.0)(0.06)] \\ &= 2.25 \times 10^{-2}\ . \end{aligned}$$

As demonstrated in the component outage case, if one were to ignore the impact from the failure of component A1 on the common-cause probability, the CCDP would be underestimated by a factor of 6.4 (i.e., 3.50×10^{-3} versus 2.25×10^{-2}).

5 SUMMARY

A part of managing nuclear power plant operations is the control of plant risk over time as components are taken out of service or plant upsets are caused by initiating events. Unfortunately, measuring risk over time proves to be challenging, even with modern PRAs and PRA tools. Early on in this paper it was asserted that the process of measuring the operational risk would satisfy three desires:

1. The risk measurement would allow the analyst to calculate the risk magnitude for a particular event or over a period of time.

2. The risk results would be consistent such that the results could be summed for an operational period of time (e.g., a single 18 month fuel cycle) to obtain a cumulative risk profile over a period of interest.

3. The risk measurement process would be tractable and represent the actual risk while still using the current modeling techniques, tools, and state of knowledge.

With these three desires in mind, this paper demonstrated a risk measurement method that can quantify operational plant risk while satisfying all three of the desires. Specifically, the calculation of a CCDP was presented for the two cases of interest: (1) component outages and (2) initiating events. While the two CCDP calculations have many similarities, the differences between the two were identified and illustrated by way of examples.

Two potential complications were identified that should be addressed when performing any type of CCDP calculation. The first complication, determining the appropriate nonrecovery probabilities to be applied to either (1) failed or inoperable component or (2) initiating events, addresses the possibility of the plant operators preventing damage to the plant from their actions. The second complication, adjusting common-cause probabilities specific to the plant configuration, accounts for the fact that the PRA common-cause probabilities built into the model are applicable only during nominal conditions (i.e., before any components have failed or become inoperable). Calculating a core damage probability conditional upon one or more unavailable component invalidates the respective common-cause basic event probabilities. The examples illustrated the potential underestimation in CCDP when the needed modifications to common-cause probabilities are ignored. Although the examples showed underestimation errors of 2.2 and 6.4 for the cases of component outages and initiating events, respectively, errors as large as a factor of 10 have been noted in previous analyses.

In closing, a method of calculating risk levels for plant operational events has been illustrated in this paper. This risk calculation, a CCDP, relies on the availability of a PRA model. Consequently, deficiencies in the PRA model itself, including errors, limitations, scoping issues, and questions of completeness, all could cause the resulting CCDP calculations to be suspect. Investing the resources to build a risk model and then subsequently use that model as part of nuclear power plant operation obligates the users to ensure the quality of the PRA model. It is only after model quality issues have been resolved can analysts focus on the quality of operational risk calculations. The techniques discussed in this paper provide a sufficient starting point for the operational risk calculation focus.

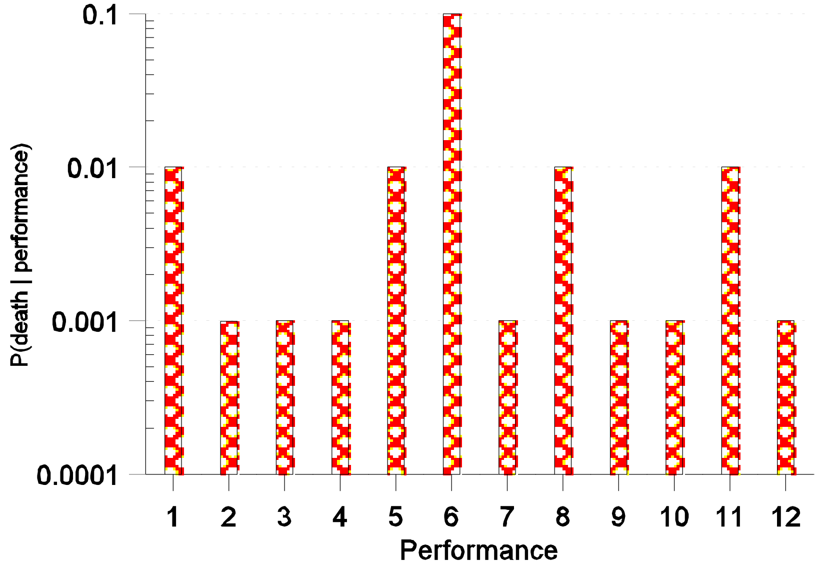

Figure 1. Magician’s probability of death risk profile.

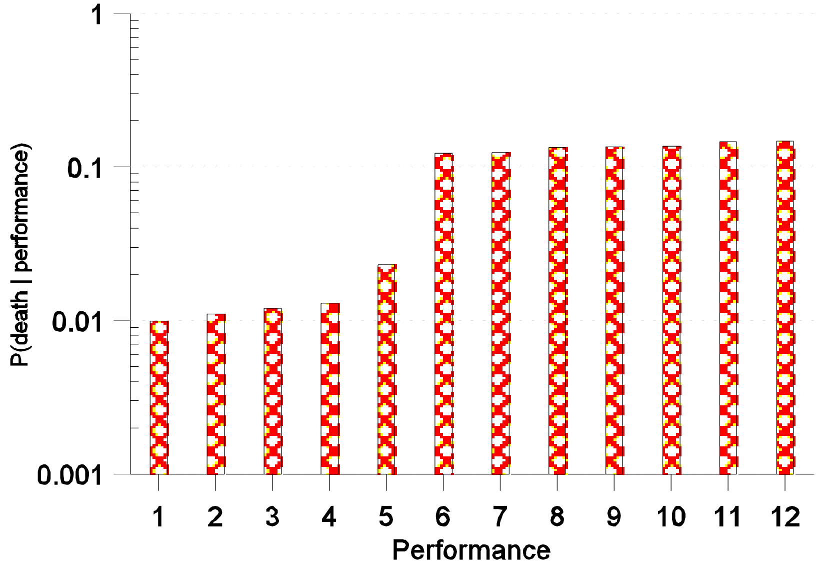

Figure 2. Magician’s cumulative probability of death risk profile.

ACKNOWLEDGMENT

This work was partially supported by the US Nuclear Regulatory Commission under DOE Idaho Field Office Contract DE-AC07-94-ID13223. This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus, product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights. The views expressed in this report are not necessarily those of the U.S. Nuclear Regulatory Commission.

The author would like to thank several colleagues in the Nuclear Risk Management Technologies branch of the Idaho National Engineering and Environmental Laboratory for their assistance leading to the development of this paper. Specifically, I would like to thank Dana Kelly, John Schroeder, Mike Calley, Tami Thatcher, and Jim Knudsen for the investigative and inquisitive help that ultimately made its way into this paper. Also, I would like to thank Jacquie Janibagian, also of the Idaho National Engineering and Environmental Laboratory, for her editorial assistance.

REFERENCES

1. Steele Jr., R. et al., *Gate Valve and Motor-Operator Research Findings*, U.S. Nuclear Regulatory Commission, NUREG/CR-6100, Washington D.C., 1995.

2. Knapik, M., editor, *Inside NRC*, "Penetration Seal Problem at Maine Yankee Challenges NRC's Position," McGraw-Hill Companies, Inc., New York, NY, April 28, 1997.

3. Fleming, K. N., *Risk-Informed Decision Making*, "Validation of PSAs for Use in Risk Monitoring Applications," American Society of Mechanical Engineers, PVP-Vol. 35B, July 1997.

4. Bain, L. J. And M. Engelhard, *Introduction to Probability and Mathematical Statistics*, Duxbury Press, Belmont California, 1992.

5. Mosleh, A., *Procedure for Analysis of Common-Cause Failures in Probabilistic Safety Analysis*, U.S. Nuclear Regulatory Commission, NUREG/CR-5801, Washington D.C., 1993.

6. *Reliability Engineering and System Safety*, "Special Issue on Dependent Failure Analysis," Vol 34, No. 3, 1991.

7. Fujita, Y., *Reliability Engineering and System Safety*, "Human Reliability Analysis: A Human Point of View," Vol 38, No. 1-2: 71-79, 1992.

8. Swain, A. D. and H. E. Guttman, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Applications*, U.S. Nuclear Regulatory Commission, NUREG/CR-1278, Washington D.C., 1983.

9. Hall, R. E., J. Wreathall, and J. R. Fragola, *Post Event Human Decision Errors: Operator Action/Time Reliability Correlation*, U.S. Nuclear Regulatory Commission, NUREG/CR-3010, Washington D.C., 1982.

10. Carolina Power and Light Company, *Brunswick Steam Electric Plant Units 1 and 2 Individual Plant Examination*, Raleigh, North Carolina, August 1992.

11. Russell, K. D, et al., *Systems Analysis Programs for Hands-On Integrated Reliability Evaluations (SAPHIRE)*, U.S. Nuclear Regulatory Commission, NUREG/CR-6116, Washington D.C., 1994.